TELECOMMUNICATIONS

OVERVIEW

The telecommunications industry is not immune from the Y2K threat. Y2K-related problems in telecommunications could have serious consequences for both national and economic security. One-third of all electric power controls, the nation's financial transactions and over 90% of defense communications rely on the smooth functioning of public telecommunications. Telecommunications also make possible the remote control of pipelines and transportation systems like air traffic control.

The 99.9% availability of telecommunications in the U.S. can make it easy to forget how much we depend upon this critical infrastructure.[1] However, the failure of AT&T's frame relay system in April 1998 and the loss of PanAmSat's Galaxy IV satellite in May 1998 remind us just how much we take telecommunications for granted. When AT&T's nationwide frame relay system for data transmission crashed, one bank lost over 1000 ATM sites and a national retailer experienced problems in over 2300 stores. When Galaxy IV disconnected 40 million people from their pagers, the effect was felt strongly throughout the economy, including healthcare which could not page critical personnel. While these failures were not Y2K related, some think they are indicative of the types of inconveniences that may result from the millennium rollover.

THE TELECOMMUNICATIONS INDUSTRY IS NOT IMMUNE FROM THE Y2K THREAT.

Our critical dependence upon communications certainly suggested an industry wide response. However, fears of competition and liability prevented a formal coordinated industry-wide approach until late in 1998.

Telecommunications used to mean switched voice communications. However, the synthesis of computers and telecommunications has broadened the way in which we think about telecommunications. The public switched network (PSN) can be defined as any switching system or voice, data, or video transmission system that is used to provide communication services to the public (e.g., public switched networks, public data networks, private line services, wireless services, wireless systems, and signaling networks).[2] Many layers of hardware and software enable the seamless communications, which allow us to make phone calls, surf the web, and transact business.

The PSN can be divided into three components:

- PSN elements

- support systems (operations, administrative and maintenance systems of the service providers)
- customer premise equipment

Public Switched Network Elements

Public switched network elements include many different devices (any one of which can have Y2K problems) that connect calls between networks. Switches, the most common telephone equipment, establish connections between two telephones when a call is made, with multiple switches required for long distance calls. Switches record the starting and ending times of a call, including the day and the year (which is necessary for calls that cross time zones). If some of the switches used in placing a call are Y2K compliant and others are not, or if the renovations are not performed in a consistent way for the different types of switches made by different manufacturers, the systems may not be able to work together.

Getting a basic dial-tone at midnight on January 1, 2000 is less likely to be a problem than disruptions in billing…

Support Systems

In testimony before the Committee Dr. Judith List, Vice President-Integrated Technology Solutions at Bellcore, explained that there is little date sensitive information in the fundamental call processing or data routing capabilities of networks. "Where we do see date sensitive information is in the operations, administration, and maintenance functions of networks," she said. Examples of these types of functions include billing, provisioning of services, network surveillance and maintenance, and other network management and administration functions.

The disruption of a carrier's operations, administration, and maintenance functions could cause some confusion for consumers with inaccurate billing and delays in the service requests. There is a concern that a buildup of errors could eventually begin to degrade service.[3]

According to a report from a high level federal advisory committee released September 10, 1998, Y2K problems could impact telecommunications in the following ways:

- ***Platform operation (hardware).*** *Hardware clocks may not recognize the year 2000.*
- ***Operating system functionality.*** *Date functions may return the wrong year to applications*
- ***Scheduling of events.*** *Errors in calendar dates can prevent scheduled events (e.g., report updates, testing, designing, provisioning, or billing) from running and can result in incipient failures.*
- ***Historical data.*** *Historical data may not be available from 1999, or 1999 may be re-ordered, with events occurring in 1999 sequenced after 2000.*
- ***Sorting and searching algorithms.*** *Dates after 1999 will be ordered before 1999; searching algorithms intended to include*

dates in 2000 (e.g., "Where date > 1997") will exclude them instead.

- ***Password expiration.*** *All passwords may expire (which would prevent authorized users from performing legitimate functions), or they may never expire (which could diminish the protection offered by password aging).*[4]

Customer Premise Equipment

Customer premise equipment (CPE) is also vulnerable to Y2K problems. CPE includes:

- Private branch exchange equipment (PBX)
- telephone equipment
- cellular phones
- fax machines
- private data networks
- public service answering points

Many small and medium sized businesses may not be aware that their privately owned communications equipment may fail because of Y2K problems. If businesses do not take a proactive approach by contacting vendors and obtaining the manufacturer's compliance information, they could have difficulty maintaining normal business functions due to the failure of their own communications equipment. The good news is CPE will not cause disruptions in the public network. However the economic impact on businesses with failed telecommunications systems may be equally as damaging.

According to the Gartner Group, networking equipment produced before 1996 has only a 50% chance of transitioning to the year 2000 without needing to be upgraded or replaced. Gartner also cautioned that local area networks (LANs) can be impacted by Y2K in a number of different ways including total failure and denying management access.[5] In view of their projection that 20% of the web servers installed prior to 1997 could fail to function properly through January 2000, the Gartner Group also warned disruptions might ultimately deny 5 percent of Internet user connectivity. Gartner is also projecting that 90% of web users could experience delays. In addition, 30% may find sites unreachable.

Competition for resources in January 2000 may make it difficult for small and medium-sized business to secure help. It is imperative that businesses and other organizations make communications a priority now.

Y2K INITIATIVES IN TELECOMMUNICATIONS

Numerous Y2K initiatives are currently underway in the telecommunications industry, including strong efforts by the Federal Communications Commission (FCC), the Network Reliability and Interoperability Council (NRIC), the Telco 2000 Forum and Alliance for Telecommunications Industry Solutions (ATIS), the National Communications Systems (NCS), and the President's National Security Telecommunications Advisory Committee (NSTAC).

The FCC

Since 1934, the FCC has regulated interstate and international communications, including radio, television, wire, satellite and cable. In July 1997, the NRIC, the FCC's federal advisory committee presented its findings and recommendations on the implementation of the Telecommunications Act of 1996 in a report entitled Network Interoperability: The Key to Competition. The report observed that "*interconnectors must ensure that their year 2000 conversion efforts are compatible.*" [6] However, NRIC made no specific recommendations for an industry-wide response to the problem.

In the summer of 1997, the Y2K problem was viewed as a due diligence effort, which only needed to be addressed by individual companies. There did not appear to be a role for the FCC or a need for a coordinated industry-wide response the Y2K problem. The lack of strong national leadership made it very easy to defer the problem. Commissioner Michael Powell was appointed to the FCC in December 1997. In his role as the FCC Defense Commissioner, he began an aggressive Y2K awareness outreach to the industry.

"*Despite carriers' best efforts to correct Y2K problems and carrier assurances that telephone service will be available on January 1, 2000, the FCC, most industry analysts, and even some carrier representatives conceded that some failures are still likely to occur.*"[7] However, the types of problems that could result remain unclear.

In March 1998, Senator Jon Kyl wrote to the Chairman of the FCC and expressed his concern about the absence of an industry-wide telecommunications effort to test for interoperability, or an accurate assessment of the industry of how Y2K may affect the Public Network (PN).[8] Senator Kyl also suggested that if NRIC was tasked by the FCC, it could produce an accurate and much needed assessment of how the Y2K problem could affect the PN. This assessment could look beyond the traditional switched network and consider other communication technologies including cellular and satellite among others. Such a report could well provide the basis for building contingency plans to ensure that communications vital to national and economic security could be maintained.

On April 28, 1998, before the Senate Commerce Committee, FCC Chairman William Kennard testified that the NRIC would be asked to examine the implications of Y2K on communications. On July 30th, a day before presenting testimony to the Y2K Committee, the FCC announced that Michael Armstrong, CEO of AT&T, would chair the newly re-chartered federal advisory group to look at Y2K. The NRIC met to propose a comprehensive plan examining three main areas:

- Y2K Impact on the Networks
- Y2K Impact on Customer Premise Equipment
- Network Reliability.

Telco 2000 Forum

One of the earliest and best-organized efforts to test for interoperability in the PN was the Telco Year 2000 Forum. Collectively representing about 145 million access lines, The Forum diligently sought to overcome the complexity of sharing information and antitrust concerns in the highly charged legal atmosphere of 1997 and 1998. The Forum, a voluntary group of eight local exchange carriers, was the first telecommunications initiative to begin identifying possible problems of interoperability. The Forum members include:

- Ameritech Corporation
- Bell Atlantic
- BellSouth
- Cincinnati Bell
- GTE
- SBC
- Southern New England Telecommunications Corporation
- US West

In an effort to reduce the possible risk of network failures, the Forum began testing in July 1998 and completed testing in January 1999. The Forum completed 1700 tests and found only seven problem areas, five of which have already been remedied. The Forum tested 16 separate configurations of network elements and data transactions and 40 unique network management configurations. These test configurations were made up of 82 commonly used telecommunications products from 21 suppliers. The Forum specifically examined the impact of Y2K fixes and interoperability on:

- Emergency services
- Basic, enhanced, and intelligent services
- Network management systems
- Data networks

The tests were concluded successfully at the end of 1998. A report is expected by the end of January 1999. The early initiative of the Forum and its commitment to business continuity will play a major role in alleviating public concern.

According to expert testimony from Gerry Roth of GTE, "*Despite the fact that this network cannot be 100 percent tested in advance of the Year 2000, we believe our individual and collective actions in Year 2000 remediation and subsequent test and validation provide a basis for continued confidence that the telephone and data networks will continue to operate and provide the outstanding services we have come to expect.*"[9]

Alliance for Telecommunications Industry Solutions

On January 4, 1999 ATIS began scheduled internetwork interoperability testing to evaluate the impact of the Year 2000 date change on the PSN. Companies participating in the testing include Ameritech, US West, GTE, AT&T and Sprint, as well as six wireless service providers (Aerial Communications, AirTouch, AT&T Wireless, Bell Atlantic Mobile, BellSouth and SBC).

Planning and implementation of the testing procedures began several months ago. Efforts included identification of the test's scope, generation of appropriate test scripts, and obtaining participants to donate lab equipment and the appropriate resources. Interconnected services to be tested on the network include toll free services; Local Number Portability (LNP); the Government Emergency Telecommunications System (GETS); and wireline-to-wireless and wireless-to-wireline interconnections.

All testing is being conducted offline to ensure no disruption of existing services to the PN. This testing effort will be accomplished by rolling forward the dates of the interconnected switches in a laboratory environment to simulate the following date rollovers:

- December 31, 1999 to January 1, 2000
- February 28 to February 29, 2000
- February 29 to March 1, 2000
- December 31, 2000 to January 1, 2001

During each simulated rollover, the signaling network will be monitored to ensure that the PN responds in a satisfactory manner.

ATIS will be testing the internetworking aspects of the PN. ATIS has designed special test scripts that will focus on time - critical network events on 31 December – 1 January to model and monitor potential network congestion and the transmission of voice and data from local exchange to inter-exchange carriers, ‘‘800’’ number access, and network management and control. Year 2000 testing will continue through February 12, with results made publicly available to interested parties on April 14, 1999.

ASSESSMENT

During 1998, there were no publicly released comprehensive studies or assessments of how Y2K could affect the telecommunications infrastructure. However, it is generally believed that Y2K will not cause prolonged disruptions. The absence of any comprehensive assessment sparked considerable uneasiness among business sectors and the public in general. The general view was that companies were working hard to address Y2K, but little factual information was available.

On January 14, 1999, NRIC released its preliminary assessments demonstrating that the telecommunications industry was meeting the Y2K challenge. NRIC estimates that the majority of the industry is on target to meet its self-imposed goal of Y2K readiness by June 1999. According to the FCC Advisory Committee, local, exchange carrier, long distance carrier and small telephones companies all seemed to be making good progress. However, small phone companies tend to lag approximately 10-15% behind larger local exchange carriers in fixing Y2K problems. The local exchange companies participating in the NRIC (approximately 99% of all the switched access lines in the U.S.) were projecting to have completed 76% of their Y2K renovations by Decem-

ber 1998. The three major long distance carriers participating in NRIC--AT&T, MCIWorldcom and Sprint--represent 82% of the market revenues. These companies are projected to have reached 81% readiness by December 1998. The NRIC assessment is an important first step.

Rural Telephone Companies

The readiness of the 1271 small companies, who provide about 1% of the access lines in the U.S., remains unclear. Some people within the rural telephone companies, contrary to popular press, pride themselves on maintaining the latest equipment. Some rural companies, for example, claim to have been the first to offer digital switching. Approximately 75% of the rural market is already scheduled for Y2K upgrades. Only 2% are not expected to be Y2K ready.[10]

Satellite Communications

Ramu Potarazu, Chief Information Officer (CIO), INTELSAT, testified before the Committee that communications satellites do not reference a time and a date; rather, a satellite references what is commonly referred to as ''satellite local time,'' that is a reference to the sun. When there is a technological reference to the sun, there usually is no reference to a specific year. INTELSAT's own analysis found that the primary problems reside in ground systems that fly, command and control, and monitor satellites.[11]

INTELSAT expressed concern about ground station users who have computer systems that may not have been upgraded over the last 10 or 15 years. According to INTELSAT, these users may have a more limited knowledge of computers because they only repair the computer system when it breaks. They may or may not be fully aware of the Y2K issue, and they may or may not be remediating any Y2K issues. The users that have outdated systems do not have money to remediate any Year 2000 issues and sometimes don't even have the money to recognize that they have a Y2K problem. Many of the earth stations throughout the world have several hundred pieces of computer equipment from various manufactures that control their ability to receive telecommunications information. For example, if antenna control units fail the antenna could not point to the satellite and no information could be sent or received.

"A significant part of INTELSAT's international communications is a two-way communication that uses an INTELSAT satellite between country A and country B. If country A's ground network is Year 2000 compliant; and INTELSAT, being the supply chain in the middle, is also compliant; and country B's ground network is not Year 2000 compliant, then you will have a failure of the complete chain."[12]

Cable, Mass Media and Wireless

Not much is known about the state of the cable, mass media or wireless industries. The FCC's Cable Bureau is in the second phase of its survey. The survey was sent to companies accounting for approximately 78

percent of the market share of cable subscribers. The first survey began in April 1998 and found that while most of the companies surveyed had started assessments, there was little progress in remediation. In November 1998, the Cable Bureau began its second survey that covers about 90% of all cable subscribers. Response should be back and assessed some time in the first quarter of 1999. It is also expected that the Mass Media and Wireless Bureaus will have completed initial assessments by the first quarter of 1999.

It is critical that contingency and disaster recovery planning and training be implemented.

CONCERNS

The Committee has three outstanding concerns in communications:

- increased contingency planning among carriers
- increased attention to Y2K security concerns
- international communications

Contingency Planning

Carriers have undertaken massive code corrections, which will be in place by the end of 1998. The large number of code corrections increase the possibility of disruptions from the introduction of new errors.[13] In testimony before the Committee, Judith List, Ph.D., vice president and general manager, Integrated Technology Solutions Business Unit, Bellcore noted the following:

"*Finally, there will be problems, and there is a level of uncertainty in this area that makes it difficult to predict where the problems will be. In the software industry today, the best in class companies find 95 percent of code anomalies before the software ever gets to the field. That means that 5 percent of software anomalies are found after the code is operational. Furthermore, according to the Software Engineering Institute, a new defect is introduced with every approximately 4 1/2 fixes of software code. Both of these statistics suggest that, given the pervasiveness and extent of Year 2000 elements, there will be problems. Furthermore, Y2K contingency planning and disaster recovery needs to address plans differently than traditional business continuity plans because backup systems are likely to have the same Year 2000 problems, issues may be more widespread across a number of industries, and problems may last for a longer period of time.*

In October 1997, the President's Commission on Critical Infrastructure Protection expressed concerns*: "The unbundling of local networks mandated by the Telecommunications Act of 1996 has the potential to create millions of new interconnections without any significant increase in the size or redundancy of network plants. Unbundling will be imple-*

mented at a time of rapid and large-scale change in network technologies. The interaction of complexity and new technologies will almost certainly expand the universe of ways in which system failure can occur, and, unlike natural disasters, there is no assurance that such failures will be localized."[14]

Telecommunications in the U.S. has one of the most highly developed systems of infrastructure assurance. In 1963, the NCS was created to ensure the federal government has enduring communications. Composed of 23 federal agencies, the NCS works closely with the telecommunications industry and maintains a coordinating center to resolve failures in the networks that could impact national security or emergency preparedness.

The NCS works closely with the National Security Telecommunications Advisory Committee (NSTAC), an advisory committee created in anticipation of the AT&T divestiture. Composed of 30 chief executive officers from telecommunications, information technology, aerospace and banking companies, the NSTAC makes recommendations to the President on issues critical to protecting the U.S. communications infrastructure. In September 1998, the NSTAC released the first report that examined the impact of Y2K on the assurance of national security and emergency preparedness communications. The NSTAC report noted that *"no organization, either private or government could offer a guarantee of total Y2K problem eradication from its networks, services, or systems. Additionally, these organizations could not offer guarantees of the adequacy of Y2K internetwork interoperability testing."*[15]

In July 1998 the NSTAC testified about the findings of its widespread outage report and highlighted the fact that the industry has had limited experience with systemic, widespread network failures. Both the NCS and the NSTAC believe that the probability for Y2K-related widespread outages is extremely low. However, because of our reliance on communications the cost would be extraordinarily high for commerce and defense. In testimony before the Committee, NSTAC expressed concern about the lack of an industry-wide plan to facilitate intercarrier coordination for recovering from a widespread outage of this nature. Most carriers have internal plans and processes for maintaining the integrity of their own networks. Looking further at contingency planning and recovery from a widespread outage, the NSTAC questioned whether existing communication and coordination mechanisms among service providers were adequate for efficient reconstitution of service. It was unclear whether the existing agreements, communications systems, and coordinating mechanisms in the industry could mitigate a severe widespread service outage.

During reconstitution, a means of communication and coordination between and among critical centers would be indispensable. The NCS works closely with the industry and is uniquely positioned to collect net-

work outage information for Y2K disruptions. [16]

As part of its normal contingency efforts, the NCS maintains a private communications network, which is independent from the PN and provides connectivity to the FCC, all of the regional Bell operating companies, GTE, Sprint, and switch manufacturers. In preparing for Y2K and other threats to the communications infrastructure, the NCS is considering expanding its network to include the Critical Infrastructure Assurance Office, and the National Infrastructure Protection Center. The private network could facilitate reconstitution efforts in the event of serious disruptions. As an additional backup, the NCS maintains high frequency (HF) radio communications with major telecommunications providers and can also access over 1000 HF radio sites around the world.

Chairman Bennett remained concerned that the administration was not developing the necessary policy to respond to an unanticipated Y2K disruption in the U.S communications infrastructure. In August 1998, Senator Bennett wrote to the Director of the Office of Science and Technology Policy (OSTP), and asked what role the Joint Telecommunications Resources Board (JTRB)[17] would play in the event of a Y2K-related emergency. The Assignment of National Security Emergency Preparedness Telecommunications (Executive Order 12472), tasked the Director of OSTP to maintain a JTRB to advise the President on the emergency allocation of telecommunications resources. The JTRB met in January 1999 for the first time in several years to determine how it might respond to a serious Y2K related event in communications.

Security

The Committee has repeatedly expressed concern about the number of code corrections that are taking place in foreign countries and the long-term security risks that this could cause for information assurance in the U.S. In response to Committee questions about the threat of malicious code, Dr. List responded:

"There is the possibility that security risks can be introduced into any code that is being remediated, not just code that is corrected in foreign countries. Programmers can, for example, introduce trap doors or back doors for non-malicious reasons, for example, to make it easier for them to maintain the code. These trap doors or back doors can then be used for other purposes to obtain unauthorized access to the software program. In other instances, security problems can be introduced for directly malicious purposes during the code remediation process. To date, I know of no easy way to assess code to ascertain the existence of these types of security risks. It requires labor intensive examination of the code, line by line. Companies can work to protect themselves from such risks by conducting adequate due diligence of employees, contractors, and service providers that they may hire to remediate Y2K

problems. In addition, implementing various policies (such as code inspections) to monitor the code remediation process also can help reduce risk."[18]

International Communications

Today global telecommunications is a growing $800 billion industry. Industry analysts note that 75% of all traffic originates or terminates in one of six countries: France, Germany, Italy, Japan, U.K. and the U.S. In addition, 90% of all call traffic comes from 20 countries. Forty percent of the global traffic touches the U.S., 20% Europe, and 15% through Asian hubs.[19] Telecommunications revenues in the U.S. are about $300 billion a year, with the majority of revenues coming from the provision of services.

At the United Nations' "National Y2K Coordinators Meeting" on December 11th 1998, the International Telecommunication Union's (ITU) Year 2000 Task Force outlined global efforts to ensure Y2K readiness in telecommunications.

The ITU established a Y2K task force in March 1998 to raise the awareness of operators and carriers by providing information on potential Y2K problems. The ITU considers one of the greatest obstacles to global readiness is the lack of awareness and action at the governmental level to pressure telecommunications operators to share information about their Y2K readiness. Part of the ITU's effort has been to recommend compliance standards and also promote the sharing of information. In addition, the ITU has encouraged the sharing of Y2K readiness information with customers. The ITU has had three main goals:

- promote Y2K best practices
- facilitate global interoperability testing
- provide specific guidance on business continuity planning.

The ITU's global assessment is somewhat sketchy at this point. However, according to the ITU, the U.S., Japan, China, Germany, France and the U.K. account for 53% of wireline infrastructure, and all are reported to have Y2K programs in place. The ITU task force also pointed out that 20 territories accounted for 80% of the world's wirelines, but there were still no details from Italy, Taiwan (Republic of China) or Ukraine. Throughout the first quarter of 1999, the ITU will organize workshops as needed in specific locations including Russia, India and Asia, to promote awareness and to increase knowledge of Y2K readiness.

Some initial testing in September 1998 did not uncover any specific Y2K problems. However, the lack of information about the readiness of global communications remains a serious concern. U.S. carriers are concerned that if foreign companies are not prepared, call completion could be impacted.